F-S-07-01：用户无法登录

典型现象

- 输入正确的用户名和密码后，页面提示"用户名或密码错误"、"账号已锁定"或"登录失败"。
- 连续多次尝试后账号被锁定。
- 其他用户可以正常登录，仅个别账号异常。

可能原因

1. **密码错误或过期**（占比约 50%）：用户输入错误、密码过期未更新、或使用了旧密码。
2. **账号被锁定**（占比约 25%）：多次尝试失败触发锁定策略，或管理员手动锁定。
3. 后端程序未正常打开（占比约 25%）：后端程序有时候关闭导致接口调取不通

排查思路

1. **确认账号状态**：在 WMS 后台"用户管理"中查询该账号，查看状态（启用/禁用）、锁定标志、密码过期时间。
2. **重置密码测试**：管理员重置该账号密码后尝试登录。若成功，原因为密码错误或过期。
3. **检查认证日志**：在应用日志中搜索 login failed 、 Authentication 、 locked 等关键词，获取具体错误信息。
4. **测试 LDAP 连通性**：如果使用 LDAP，从应用服务器 ldapsearch 或 telnet LDAP 端口（389/636），确认服务正常。
5. **验证 JWT 配置**：若使用 Token 认证，检查 Token 签名密钥、有效期、刷新机制是否正确。

保养提示

- 启用密码过期提醒：在密码过期前 7 天，登录时提示用户修改密码。
- 设置账号锁定策略（如 5 次失败锁定 30 分钟），并记录锁定日志供审计。
- 定期检查 LDAP 同步任务，确保本地用户状态与 LDAP 一致。

F-S-07-02：权限不足无法操作

典型现象

- 用户点击某个按钮或菜单时，提示“权限不足”、“无操作权限”或按钮置灰。
- 同一角色中的其他用户可以正常操作。
- 用户之前可以操作，某次升级或权限调整后失去权限。

可能原因

1. **角色未分配**（占比约 45%）：用户未关联正确的角色，或角色缺少该功能的权限点。
2. **权限缓存未刷新**（占比约 25%）：用户权限变更后，服务端或前端缓存的旧权限未更新。
3. **数据权限限制**（占比约 15%）：用户有权操作，但受限于数据范围（如只能查看自己仓库的订单）。

排查思路

1. **确认用户角色与权限**：在“角色管理”中查看用户关联的角色，以及该角色是否勾选了目标权限点。
2. **对比有权限的用户**：找一个能正常操作的账号，对比其角色和权限配置差异。
3. **清除并刷新缓存**：
    - 后端：重启服务或调用权限缓存刷新接口（如 /refresh-permissions ）。
    - 前端：清除浏览器缓存，退出重新登录。
4. **检查数据权限配置**：如果操作涉及部门、仓库等数据范围，确认用户的数据权限规则是否包含目标资源。
5. **查看后端日志**：测试操作时，日志中应打印权限校验过程，查找 AccessDenied 或 PermissionEvaluator相关日志，确认失败原因。

保养提示

- 定期审查角色权限配置，避免权限膨胀或缺失。
- 为重要操作记录“权限变更日志”，便于追溯谁在何时修改了权限。
- 开发环境提供“权限模拟”功能，管理员可模拟任意用户查看其权限布局。

F-S-07-03：越权访问其他仓库_数据

典型现象

- 用户 A 可以查看或操作用户 B 所属仓库的数据（如订单、库存）。
- 修改请求中的 warehouseId 或 userId 参数后，可以访问不应访问的数据。
- 安全测试或审计发现水平越权漏洞。

可能原因

1. **服务端未做数据权限校验**（占比约 60%）：接口仅校验用户登录，但未校验请求中的资源 ID 是否属于该用户。
2. **前端隐藏但接口可调用**（占比约 20%）：前端界面按钮是隐藏的，但用户直接调用后端接口（如 Postman）仍可成功。
3. **权限配置遗漏**（占比约 10%）：某些新开发的接口未集成权限框架，默认放行。
4. **缓存数据未隔离**（占比约 5%）：多租户共享缓存时，未在缓存 key 中加入租户 ID。
5. **SQL 注入或其他绕过**（占比约 5%）：攻击者通过 SQL 注入等手段绕过权限检查。

排查思路

1. **重现越权路径**：使用两个不同仓库的账号（或不同用户的 token），尝试访问对方的数据接口（如 /order/detail?orderId=xxx ）。
2. **审查接口代码**：检查控制器方法是否添加了权限注解（如 @RequiresDataPermission ），是否手动校验了warehouseId 与当前用户绑定。
3. **检查参数校验**：确认接口不会仅相信前端传递的 userId 或 warehouseId ，而是从 token 或 Session 中获取当前用户身份。
4. **测试边界值**：使用无效 ID（如 -1、0 或超大值）调用接口，看是否返回异常数据。
5. **扫描未授权接口**：使用自动化工具（如 Burp Suite）遍历常用接口路径，检测哪些接口未做鉴权。

保养提示

- 强制要求所有业务接口在服务端进行数据权限校验，校验逻辑应基于登录用户的身份（而非前端参数）。
- 定期执行安全代码审计和渗透测试，重点检查新增接口。
- 对敏感操作（如删除订单、修改库存）增加二次验证（如输入密码）。

F-S-07-04：API 被恶意调用

典型现象

- 某个接口在短时间内被大量请求，导致服务响应变慢或崩溃。
- 日志中出现异常的请求来源 IP 或参数（如批量查询用户信息）。
- 业务数据被篡改或外泄。

可能原因

1. **无鉴权或鉴权薄弱**（占比约 50%）：接口未要求 Token、API Key 或签名，可以直接调用。
2. **Token 泄露**（占比约 25%）：前端代码中硬编码了 Token，或 Token 未设置合理过期时间。
3. **缺少限流措施**（占比约 15%）：接口没有设置访问频率限制（Rate Limit），攻击者可以暴力调用。
4. **参数可枚举**（占比约 10%）：接口使用自增 ID 作为资源标识，未做防猜保护。

排查思路

1. **分析异常调用模式**：查看 API 日志，统计单位时间内请求 IP、参数值、请求路径，找出异常集中点。
2. **检查接口鉴权配置**：确认接口是否要求携带 Token 或签名。若没有，立即补充鉴权。
3. **检查 Token 有效期**：验证是否存在永不过期的 Token，或 Token 存储在前端 localStorage 未加密。
4. **实施限流策略**：在网关或应用层配置 Rate Limit（如每 IP 每秒 10 次）。观察限流后异常是否减少。
5. **防止参数枚举**：将资源 ID 改为 UUID 或随机字符串，避免使用自增数字。

保养提示

- 所有对外/对内 API 必须强制鉴权，推荐使用 OAuth2 或 JWT 并设置合理过期时间。
- 部署 API 网关（如 Kong、Spring Cloud Gateway），统一管理限流、黑白名单和监控。
- 定期轮换 API 密钥和 Token，并对异常 IP 自动加入黑名单。

F-S-07-05：操作日志未记录

典型现象

- 用户执行了关键操作（如删除订单、修改库存），但系统审计日志中查不到记录。
- 事后追溯问题时缺少操作轨迹。
- 合规检查发现日志缺失。

可能原因

1. **日志配置错误**（占比约 45%）： Logback/log4j2 配置中未设置对应包的日志级别，或日志未输出到文件。
2. **异步队列丢失**（占比约 25%）：操作日志通过消息队列异步写入，队列积压或消费者故障导致日志丢失。
3. **数据库日志表写入失败**（占比约 15%）：将日志存储在数据库中，但数据库连接失败或表空间满，写入被静默忽略。
4. **代码中未埋点**（占比约 10%）：开发人员忘记在关键操作处添加日志注解或手动记录。
5. **日志级别过滤**（占比约 5%）：生产环境日志级别设为 ERROR，而操作日志为 INFO，导致未输出。

排查思路

1. **检查日志配置文件**：确认是否配置了 AsyncAppender ，以及 additivity 设置。查看 logback.xml 或 log4j2.xml 。
2. **测试手动记录**：在代码中临时添加 log.info("test log")，观察是否输出到目标文件。若不输出，检查日志路径权限和配置。
3. **查看日志队列状态**：如果使用 MQ 写日志，检查队列深度、消费者状态、死信队列中是否有未处理消息。
4. **检查数据库日志表**：连接数据库，查看日志表的大小和是否可写。尝试手动插入一条记录，确认权限和空间。
5. **审查代码**：搜索关键业务方法，确认是否有 @Log 注解或显式日志调用。
6. **查看错误日志**：搜索 log 相关错误（如 LoggingException 、 Appender ），确认是否有写入失败记录。

保养提示

- 统一使用 AOP 切面记录关键操作日志（入参、出参、耗时、操作人），减少手工埋点遗漏。
- 日志存储建议：重要操作日志同步写入数据库，并配置双写本地文件作为备份。
- 定期检查日志存储空间，并设置日志保留策略（如保留 180 天自动清理）。